UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

EDWARD QUINN and MONIQUE LESLIE, on behalf of themselves and all others similarly situated, Plaintiffs, v. RICHMOND UNIVERSITY MEDICAL CENTER, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Edward Quinn and Monique Leslie (collectively "Plaintiffs"), by and through their attorneys, hereby bring this Class Action individually and on behalf of all others similarly situated (collectively, "Class members"), against Defendant Richmond University Medical Center ("Defendant"). Plaintiffs complain and allege the following upon personal knowledge as to themselves and upon information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach that occurred on May 6, 20223 which affected Defendant's inadequately protected computer systems and/or network, and which did result in the unauthorized access to, and subsequent acquisition of, approximately 674,033 individuals' personally identifiable information ("PII") and personal health information ("PHI") (hereinafter the "Data Breach").

2. PII and PHI includes, among other sensitive information, confidential medical information, names, date of birth, addresses, health insurance plan information, payment card information, Social Security numbers ("SSNs"), medical record numbers, health plan beneficiary numbers, treatment information, diagnosis information, and/or other medical information.

3. Defendant is a national award-winning healthcare facility and teaching institution.[1]

4. As a condition of receiving services, Defendant's patients are required to provide and entrust Defendant with sensitive and private information, including PII and PHI. Patients thereafter provide their PII and PHI to Defendant with the reasonable expectation that their sensitive information will be kept confidential and safe from unauthorized disclosure.

5. By taking possession and control of their information, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' PII and PHI from unauthorized disclosure.

6. Defendant also has a duty to adequately safeguard its patients' sensitive and private information under industry standards and duties imposed by statutes, including the Health Insurance Portability and Accountability Act ("HIPPA"), Section 5 of the Federal Trade Commission Act ("FTC Act"), and other relevant laws and regulations.

7. Defendant breached its duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

8. On or about May 6, 2023, Defendant discovered a cyberattack that resulted in unauthorized access to its network.[2] Defendant opened an investigation into the incident to determine whether patient data was leaked as a result.[3] Defendant also retained leading cybersecurity experts to assist in the investigation.[4]

9. While Defendant claimed to have discovered the breach on May 6, 2023, it did not notify victims of the breach until a year and a half later, in December 2024, when it confirmed

[1] https://www.linkedin.com/company/richmond-university-medical-center.
[2] https://www.rumcsi.org/wp-content/uploads/2024/05/Richmond-University-Medical-Center-Data-Security-Incident33486493.1.pdf; *see also* https://www.rumcsi.org/wp-content/uploads/2024/12/Richmond-University-Medical-Center-Notifies-Potentially-Affected-Individuals-of-Information-Security-Incident32482687.1.pdf.
[3] *Id.*
[4] *Id.*

that cybercriminals had accessed its systems and the personal information of its patients, and began to mail breach notification letters to victims, including Plaintiffs.

10. Presently, Defendant has offered no assurance to Plaintiffs and Class members that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

11. The information compromised in the Data Breach was disclosed by Defendant to be patients' full names, Social Security numbers, dates of birth, driver's license and/or state identification numbers, other government identification numbers, health insurance plan information, medical treatment/diagnosis information, financial account information, credit or debit card information, user credentials, and biometric information.[5]

12. The exposure of a person's PII and PHI through a data breach substantially increases that person's risk of identity theft, fraud, misappropriation of health insurance benefits, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts, health records, and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

13. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII and/or PHI was accessed and disclosed. Plaintiffs and Class members are now at a substantially increased risk of experiencing misuse of their PII/PHI in the coming years. This action seeks to remedy these failings and their consequences.

14. Plaintiffs, on behalf of themselves and all other Class members whose PII/PHI was exposed in the Data Breach, assert claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, unjust enrichment, invasion of privacy, and breach of California

[5] https://www.rumcsi.org/wp-content/uploads/2024/12/Richmond-University-Medical-Center-Notifies-Potentially-Affected-Individuals-of-Information-Security-Incident32482687.1.pdf.

state consumer protection laws and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

15. Plaintiff Edward Quinn is a natural person and citizen of New York. Plaintiff received notice of the breach from Defendant stating that his personal information was compromised in the Data Breach.

16. Plaintiff Monique Leslie is a natural person and citizen of New York. Plaintiff received notice of the breach from Defendant stating that the personal information of her and her two minor children was compromised in the Data Breach.

17. Plaintiffs received medical treatment from Defendant and were required to submit their personal information to Defendant as a condition of those services and treatment, including their names, addresses, dates of birth, contact information, driver's license information, Social Security number, and full health and financial information.

18. Defendant Richmond University Medical Center is a not-for-profit New York healthcare facility and teaching institution, with its principal place of business at 355 Bard Avenue, Staten Island, New York 10310.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), and the amount in controversy exceeds the $5,000,000 jurisdictional minimum of the Class Action Fairness Act, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's states of citizenship.

20. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this jurisdiction, maintains its principal place of business in this jurisdiction, regularly conducts business in this jurisdiction, and the acts and omissions giving rise to Plaintiffs' claims emanated from within this jurisdiction.

21. Venue is proper in this jurisdiction because Defendant's principal place of business is in this County and the acts and omissions giving rise to Plaintiffs' claims emanated from within this jurisdiction.

FACTUAL ALLEGATIONS

Defendant Stores Patient PII/PHI

22. Defendant is a healthcare facility and teaching institution in New York and is nationally recognized for its services as a Level 1 Trauma Center and designated Stroke Center. Defendant provides "acute, medical and surgical care, including emergency care, surgery, minimally invasive laparoscopic and robotic surgery, gastroenterology, cardiology, pediatrics, podiatry, endocrinology, urology, oncology, orthopedics, neonatal intensive care and maternal health" and behavioral health services.[6]

23. As a condition of treating its patients, Defendant requires that its patients entrust it with sensitive and private information such as patient names, dates of birth, addresses, Social Security number, medical history, and financial information in the ordinary course of its business. Upon information and belief, Defendant may also collect other sensitive personal and health information such as PII/PHI. Defendant collects and maintains the aforementioned information to provide medical services to donors.

24. Upon information and belief, Defendant may also receive private and personal information from individuals within its patients' "circle of care," such as family members, close friends, referring physicians and/or other doctors.

25. Defendant's applicable privacy policy demonstrates that it is aware of its legal obligations to keep PII and PHI confidential and secure, and indeed promises to do just that. Defendant's privacy policy admits that it is "required by law to protect the privacy of health

[6] *Supra* n.1.

information that may reveal your identity."[7] Further, Defendant promises "[o]ther uses and disclosures not covered by this notice will be made only with your written authorization."[8]

26. In its privacy policy, Defendant acknowledges it is "required by law to notify affected individuals following a breach of unsecured protected health information."[9]

27. Despite Defendant's representations about the privacy of its patients' information, it did not employ reasonable security measures to protect its patients' PII and PHI from unauthorized disclosure as demonstrated throughout this Complaint.

28. Upon information and belief, the type of information that Defendant maintains includes, *inter alia*: patients' full name, address, date of birth, Social Security number ("SSN"), health insurance information, financial information, and medical information.

29. Due to the highly sensitive nature of the information Defendant collects and maintains, Defendant is obligated provide confidentiality and adequate security for donor safety through its applicable privacy policy, and otherwise in compliance with statutory privacy requirements.

30. In the course of their relationship, Plaintiffs and Class members provided Defendant with at least their PII and/or PHI.

31. Plaintiffs and Class members, as current and/or former patients of Defendant, relied on Defendant to keep their sensitive PII/PHI confidential and secure, to use such information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

32. On or about May 6, 2023, Defendant discovered "unauthorized access to our

[7] https://www.rumcsi.org/careers/our-mission/notice-of-privacy-practices/#:~:text=We%20may%20use%20your%20health,it%20will%20cover%20your%20treatment.
[8] *Id.*
[9] *Id.*

network that resulted in the unauthorized access to, or acquisition of, certain files by an unauthorized actor." In response, it launched an investigation and determined "certain other files may have been accessed or removed from our network on or around May 6, 2023" and then conducted a manual review that determined "at least one of those files" contained PII/PHI information.[10]

33. On or about December 19, 2024, in its notice of breach event to the Attorney General of Maine, Defendant confirmed that the information compromised in the Data Breach included patients' names, addresses, dates of birth, health insurance information, medical information, Social Security numbers.[11]

34. Simultaneously with confirmation of the Data Breach, Defendant began to notify the victims of the breach on or about December 19, 2024, a year and seven months after the attack occurred.[12]

35. Defendant's failure to promptly notify Plaintiffs and Class members that their PII and PHI was compromised placed them at a higher risk that their information will be used towards illegal means since their information was vulnerable for roughly a year and seven months without their knowledge. Due to the delay, Plaintiffs and Class members were unable to take affirmative steps to mitigate their risks of fraud and/or identity theft from the unauthorized disclosure of their PII and PHI.

36. Additionally, the breach notification letter is deficient, which quite simply informs victims that their PII and/or PHI had been compromised.

> We discovered unauthorized access to our network that resulted in the unauthorized access to, or acquisition of, certain files by an unauthorized actor. Upon learning of this issue, we immediately contained and secured the threat and commenced a prompt and thorough investigation. Our investigation was done in consultation with outside cybersecurity professionals who regularly investigate and analyze these

[10] https://www.rumcsi.org/wp-content/uploads/2024/12/Richmond-University-Medical-Center-Notifies-Potentially-Affected-Individuals-of-Information-Security-Incident32482687.1.pdf.
[11] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ca5e8f97-4e10-43c1-9fdb-bede3279bf13.html.
[12]

> types of situations to help determine whether any sensitive data had been compromised because of the incident. Although the initial forensic investigation determined our electronic health records system was not affected by the incident, the investigation subsequently determined that certain other files may have been accessed or removed from our network on or around May 6, 2023. Once the investigation determined what files may have been accessed or removed from our network, we located a copy of each file and then undertook a manual review process of those files to determine whether they contained any sensitive personal information or personal health information.[13]

37. Notably, the breach notification letter fails to adequately describe with specificity the nature of the attack and the measures taken by Defendant, if any, to prevent future attacks. Without these details, Plaintiffs and Class members are at a disadvantage to take steps to mitigate the harms resulting from the Data Breach.

38. Instead, Defendant vaguely states that they are "committed to maintaining the privacy of personal and protected health information" and does not discuss the specific actions it has implemented to address the Data Breach and to prevent a future occurrence, only referencing past actions:

> We recognize the importance of protecting your information and deeply regret that this situation occurred. We are committed to maintaining the privacy of personal and protected health information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal and protected health information.[14]

39. The mitigation efforts offered by Defendant in the breach notification letter are also wholly deficient.

40. Defendant has offered one year of credit monitoring and identity protection services, which is inadequate to redress the damage to Plaintiffs' and Class members' privacy and the imminent threat they now face and will likely continue to face for the remainder of their lives.

41. Defendant wishes to place the burden of identity protection on Plaintiffs and Class members when the blame for the access and disclosure of their PII and PHI is through no fault of their own. Rather, it is Defendant's fault.

[13] Available for download at https://www.rumcsi.org/about/, "Notice of Data Security Incident."
[14] *Id.*

42. Based on the unfortunate events described throughout this Complaint, Defendant failed to take action to prevent the Data Breach by implementing data security measures to protect its network from unauthorized breach and thereby failed to protect its patients' PII and PHI.

43. Defendant further failed timely detect the Data Breach until information was already accessed.

44. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains PII/PHI on its computer network and/or systems.

45. Plaintiffs' and Class members' PII and PHI was compromised and acquired in the Data Breach.

46. Plaintiffs further believe that their PII and PHI will continue to be available for purchase on the dark web, which is the *modus operandi* of cybercriminals.

47. Plaintiffs and Class members now face a heightened and continued threat of identity theft and other types of criminal mischief resulting from the Data Breach.

48. The long-lasting effects of the Data Breach are particularly worrisome since it affects Defendant's current and former patients, who now must live the remainder of their lives under this threat, which was preventable by Defendant.

Defendant Knew that PII/PHI is Valuable to Cybercriminals and Failed to Take Action to Prevent its Theft

49. At all relevant times, Defendant knew, or should have known, that Plaintiffs' and Class members' PII/PHI was a target for cybercriminals. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyberattacks.

50. By acquiring, collecting, and using Plaintiffs' and Class members PII/PHI, Defendant assumed legal and equitable duties created by the HIPPA, the FTCA, industry standards, contract, and statutory and common law to keep Plaintiffs' and Class members PII/PHI confidential, and to protect it from unauthorized access and disclosure.

51. Additionally, Defendant's data security obligations were of particular importance due to the steady increase over the years of data breaches targeting medical information.

52. The healthcare industry is a known target for cyber criminals. "High demand for patient information and often-outdated systems are among the nine reasons healthcare is not the biggest target for online attacks."[15] They are also more likely to pay for a hacker's ransom due to the sensitive information that they maintain and collect, and an incentive to regain access to their data quickly.[16]

53. The number of data breaches experienced by healthcare entities continues to rise. In a 2024 report, the healthcare compliance company Protenus found that there were 942 medical data breaches in 2023, leaving over 171 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[17]

54. According to Mimecast, a cybersecurity firm, 90% of healthcare organizations experienced cyberattacks in 2020.[18]

55. In fact, the last several years are marked by several high-profile healthcare data breaches including:

- Eastern Radiologists, Inc. (886,746 patients, February 2024);
- MCNA Dental (8,900,000 patients, March 2023);
- Broward Health (1,300,000 patients, January 2022);
- Morley (521,046 patients, February 2022);

---

[15] Swivel Secure, *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Oct. 29, 2024).

[16] Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/. (last visited Oct. 29, 2024).

[17] *2024 Breach Barometer*, PROTENUS, available for download at: https://www.protenus.com/breach-barometer-report (last visited Oct. 29, 2024).

[18] Maria Hernandez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988- iowa-city-hospital-suffers-phishing-attack (last visited Oct. 29, 2024).

- Regal Medical Group (3,300,000 patients, December 2022);
- Trinity Health (3,300,000 patients, March 2020);
- Shields Healthcare Group (2,000,000 patients, March 2022); and
- One Touch Point (2,600,000 individuals, July 2022).

56. An article from April 23, 2024 discussed the latest findings in Baker Hostetler's tenth annual Data Security Incident Response Report, which found that despite companies' adeptness to respond to cyberattacks from criminals, "ransomware attacks show no signs of abating…"[19] Moreover, "Combating these attacks has also been complicated by hackers' practice of constantly innovating and evolving their methods in order to get around the controls and safeguards that businesses are erecting to counter their attacks…"[20]

57. Defendant certainly knew and understood that unprotected or exposed PII/PHI in the custody of healthcare entities, like Defendant, is valuable and highly sought after by criminals seeking to illegally monetize that PII/PHI through unauthorized access.

58. Indeed, personal data such as PII/PHI is a valuable property right, leading to the purchase of said data by American companies. American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[21]

59. Consumers also place a high value on the privacy of their data. Studies confirmed that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22] Recently, more consumers

[19] Allison Grande, *Ransomware Still on the Rise Despite Better Defenses, Firm Says*, LAW 360 (Apr. 23, 2024), https://www.law360.com/articles/1827647/ransomware-still-on-rise-despite-better-defenses-firm-says (last visited Oct. 29, 2024).
[20] *Id.*
[21] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited July 17, 2024).
[22] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[23]

60. Considering the value behind PII/PHI, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

61. PII/PHI is also of high value to identity thieves, as evidenced by their practice of trading such private information including, SSNs, on the black market or "dark web." PII/PHI is a measurable commodity on the black market.[24] PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[25] In 2021, it was reported that stolen healthcare records can also fetch for as much as $1000 on the black market.[26] That price is likely much higher today.

62. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[27]

63. Another report demonstrates that cybercriminals continue to profit from ransomware attacks: "The largest ransom paid in 2023 was more than $10 million, an increase from the $8 million payment high from 2022, and the average ransom paid in 2023 was $747,651,

[23] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742.

[24] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited Oct. 29, 2024).

[25] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Oct. 29, 2024).

[26] Paul Nadrag, *Industry Voices-Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web) (last visited July 17, 2024).

[27] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

which nearly matches the average payment high that was set in 2020 during the height of the ransomware epidemic, the report noted."[28]

64. Companies like Defendant are aware that consumers value the privacy of their sensitive data such as PII/PHI and that cybercriminals continue to successfully target that data to obtain significant profits. As such, companies like Defendant remain on high alert and must act in accordance with their legal and equitable obligations to implement reasonable security measures to prevent targeted data attacks aimed at their patients' PII/PHI.

65. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII/PHI from being stolen.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

66. The theft of PII/PHI is costly for those affected. A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[29] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[30]

67. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, identity theft can happen in many ways: fraudsters can obtain and sell personal data to other criminals, or use personal data to open a new credit card or loan, open a bank account and write bad checks, apply for government benefits, take over existing debit and credit accounts, withdraw funds, and even get medical procedures.[31]

---

[28] *Supra* n.19.

[29] *Supra* n.25.

[30] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited Oct. 29, 2024).

[31] Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-

68. The Federal Trade Commission ("FTC") also warns consumers about the type of fraud that identity thieves use PII/PHI to achieve.[32] Criminals can also obtain a driver's license or official identification card in the victim's name, but with the thief's picture, use the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[33]

69. Alarmingly, a thief can use stolen medical information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[34]

70. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a week to resolve issues stemming from identity theft and some need months to a year.[35]

71. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

72. Victims of medical identity theft face another set of problems. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

---

experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited Oct. 29, 2024).

[32] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Oct. 29, 2024).

[33] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 17, 2024).

[34] *Supra* n.25.

[35] Identity Theft Resource Center, 2023 Consumer Impact Report, available for download at: https://www.idtheftcenter.org/publications/.

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected;

- Significant bills for medical goods and services not sought nor received;

- Issues with insurance, co-pays, and insurance caps;

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft;

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime;

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts;

- Phantom medical debt collection based on medical billing or other identity information; and

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[36]

73. Further complicating victims' ability to defend selves from identity theft is the time lag between when PII/PHI is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[37]

[36] World Privacy Forum, *The Geography of Medical Identity Theft* (Dec. 12, 2017), available for download at: https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

[37] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), available at: http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf

74. Plaintiffs and Class members now live with their PII/PHI exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

75. Plaintiffs and Class members now face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII/PHI.

Defendant Failed to Comply with Statutory Regulations

76. The Health Insurance Portability and Accountability Act ("HIPPA") requires covered entities to implement reasonable security measures to protect patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

77. HIPPA further prohibits the unauthorized disclosure of protected health information.

78. Defendant is a HIPPA covered entity that provides healthcare services. *See* 45 C.F.R. § 160.12. As a regular and necessary part of its business, Defendant collects and maintains PII/PHI of patients.

79. HIPPA requires Defendant to implement adequate safeguards to prevent unauthorized use or disclosure of private information such as PII/PHI by adopting the requirements set forth in the HIPPA's Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

80. Defendant is also required to report any unauthorized use or disclosure of that information, including incidents of a data breach "without unreasonable delay and in no case later than 60 days following discovery of the breach."[38] *See* 45 C.F.R. § 164.302.

81. As a HIPPA covered entity, Defendant assumed legal obligations and knew or should have known that it was responsible for safeguarding Plaintiffs' and Class members' sensitive and private information from unauthorized disclosure.

82. As set forth throughout this Complaint, Defendant did not implement the required safeguards it is required to maintain under HIPPA. Defendant did so with knowledge of its legal duties under HIPPA and of the risks associated with unauthorized access to Plaintiffs' and Class members' PHI.

83. Defendant's HIPPA violations include but are not limited to the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits. 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of PHI. 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosure of electronic PHI that is not permitted. 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPPA security standards by Defendant's workforce. 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate the harmful effects of security incidents that are known. 45 C.F.R. § 164.308(a)(6)(ii);

[38] Breach Notification Rule, U.S. Dep't of Health & Human Services, available at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry our their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI. 45 C.F.R. § 164.530(c).

84. As a result of their failure to comply with HIPPA regulations, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and injuring Plaintiffs and Class members.

85. The Federal Trade Commission Act ("FTCA") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." *See* 15 U.S.C. § 45.

86. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

87. The FTC's publication, *Protecting Personal Information*, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal patient information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[39]

88. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40]

89. The FTC further recommends that businesses not maintain private information longer than is needed for authorization of a transaction; limit access to sensitive information; require complex passwords be used on networks; use industry-tested methods for security monitor

[39] *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[40] *Id.*

for suspicious activity on the networks; and verify that third-party service providers have implemented reasonable security measures.

90. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII/PHI adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

91. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

92. Defendant failed to properly implement basic data security practices.

93. Defendant was at all relevant times fully aware of its obligations to protect donors' PII/PHI, and of the significant consequences that would result from its failure to do so.

94. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to donors' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

95. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach.

Defendant Failed to Comply with Industry Standards

96. Industry standards for healthcare providers such as Defendant exist because of the high threat of cyberattacks that target the sensitive information that they collect and maintain.

97. These practices include, but are not limited to: educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and monitoring and limited access to physical security systems.

98. Defendant failed to meet the minimum standards of any of the following: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1,

DE.CM-4, DE.CM-7, DE.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

99. Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiff and Class members.

Common Damages Sustained by Plaintiffs and Class Members

100. For the reasons mentioned above, Plaintiffs and all other Class members have suffered injury and damages directly attributable to Defendant's failure to implement and maintain adequate security measures, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

Plaintiff Quinn's Experience

101. Plaintiff Quinn is a patient of Defendant's and Data Breach victim.

102. As a condition of receiving medical treatment from Defendant, Plaintiff was required to provide private information to Defendant including his name, address, date of birth, contact information, driver's license information, Social Security number, biometric data, and full health and financial information.

103. Upon information and belief, Defendant retained Plaintiff's private information in its system at the time of the Data Breach.

104. On or about December 19, 2024, Plaintiff received a notice letter from Defendant which identified him among the victims "whose information was impacted in this cybersecurity attack."

105. The letter disclosed that information stolen included "name, address, Social Security number, date of birth, biometric information, health insurance plan information, and medical information."

106. Plaintiff is careful about sharing his private information. Plaintiff stores any documents containing private information in a safe and secure location. Plaintiff would not have entrusted his private information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

107. Plaintiff's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach. Since learning of the breach, fraudulent activity occurred on his Bank of America Credit Card in or around late December 2024.

108. Plaintiff spent time calling Bank of America customer service to assist with redressing the fraudulent activity on his card. Bank of America ended up reversing the unauthorized transaction and mailed an entirely new credit card. Plaintiff received an email notification that the mailing address to where the new card was being sent had been changed to a Bronx, New York address that he did not recognize. The unauthorized user had somehow managed to also steal and use his online bank account credentials to log onto Plaintiff's online bank portal to monitor and interfere with the mailing out of a new card.

109. In response, Plaintiff contacted Bank of America again and a new card was issued and mailed out to Plaintiff's correct mailing address. Plaintiff's password was also reset to ensure that the unauthorized user could not regain access to his account.

110. Since the announcement of the Data Breach, Plaintiff has been required to spend valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII/PHI, time he would not have had to spend but for the Data Breach.

111. As a result of the Data Breach, Plaintiff suffered actual injury including, but not limited to: (i) a substantially increased risk of identity theft and medical theft; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established

national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

112. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff's PII/PHI is still at risk of being stolen and used for fraudulent activity.

Plaintiff Leslie's Experience

113. Plaintiff Leslie is a patient of Defendant's and a Data Breach victim.

114. Upon information and belief, Defendant retained Plaintiff and her two minor children's private information in its system at the time of the Data Breach.

115. On or about December 19, 2024, Plaintiff received a notification letter in the mail from Defendant which identified her as among the victims "whose information was impacted in this cybersecurity attack."

116. The letter disclosed that information stolen included "name, address, Social Security number, date of birth, biometric information, health insurance plan information, and medical information."

117. Plaintiff is careful about sharing her private information. Plaintiff stores any documents containing private information of both her and her two children in a safe and secure location. Plaintiff would not have entrusted her private information with Defendant had she known of Defendant's failure to implement and maintain data security measures.

118. Plaintiff's PII and/or PHI, along with her two minor children, were improperly accessed and obtained by unauthorized third parties in the Data Breach. Since the breach occurred, Plaintiff has received an abnormally high number of spam calls and email messages. She has also had multiple instances of fraudulent activity on her Chime bank account during the same time period. To the best of her recollection, there were about five attempted fraudulent charges made to her bank during the time following the occurrence of the Data Breach.

119. Plaintiff spent time calling her bank to reverse the fraudulent charges and have a new debit card reissued and mailed out to her. In addition, Plaintiff has also expended considerable time monitoring both her minor children's phones for any spam calls and researching the unrecognizable numbers for those calls.

120. Since the announcement of the Data Breach, Plaintiff has been required to spend valuable time monitoring her various accounts in an effort to detect and prevent any misuses of her, or her minor children's, PII/PHI, time she would not have had to spend if the Data Breach had not occurred.

121. As a result of the Data Breach, Plaintiff suffered actual injury including, but not limited to: (i) a substantially increased risk of identity theft and medical theft; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

122. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff's PII/PHI is still at risk of being stolen and used for fraudulent activity.

CLASS ALLEGATIONS

123. Plaintiffs bring this class action individually and on behalf of all persons similarly situated, pursuant to 28 U.S.C. § 1332(d).

124. Plaintiffs seek certification of a Class as defined below and subject to further amendment:

Nationwide Class

All individuals in the United States whose PII and/or PHI was compromised in the Data Breach (the "Class").

State Subclass

All individuals residing in New York whose PII and/or PHI was compromised in the Data Breach (the "New York Subclass").

125. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

126. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

127. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of those affected by the Data Breach remains unknown, the Class size and the affected individuals' contact information is available from Defendant's business records.

128. Commonality. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;

c. Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII/PHI;

d. Whether Defendant breached its fiduciary duty to Plaintiffs and Class members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;

g. Whether hackers obtained Plaintiffs' and Class members' data in the Data Breach;

h. Whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

i. Whether Defendant invaded Plaintiffs' and Class members' privacy;

j. Whether Defendant was unjustly enriched;

k. Whether Plaintiffs and Class members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and

l. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

129. Typicality. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

130. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

131. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered

in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

132. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class members affected by the Data Breach.

133. Finally, class certification is appropriate. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

134. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

135. Defendant requires that its patients, including Plaintiffs and Class members, submit private information such as PII and PHI in the course of providing its medical services.

136. Defendant collected, acquired, and stored Plaintiffs' and Class members' private information.

137. Plaintiffs and Class members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

138. Defendant had knowledge of the sensitivity of Plaintiffs' and Class members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that healthcare entities were the target of cyberattacks in the past, and that Plaintiffs and Class members were the foreseeable and probable victims of any inadequate data security procedures.

139. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to Plaintiffs and Class members.

140. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information. Defendant also owed a duty to Plaintiffs and Class members to notify them within a reasonable time of any breach to the security of their sensitive and private information.

141. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the HIPPA, the FTCA, industry standards, and other statutory law.

142. Defendant's duty also arose from its position as a healthcare provider. As a healthcare provider, Defendant assumed a duty to exercise reasonable care in safeguarding and protecting donors' private information in its possession, custody, or control from the unauthorized disclosure of such information.

143. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

144. Defendant admitted that the PII/PHI of Plaintiffs and Class members was disclosed to unauthorized third persons as a result of the Data Breach.

145. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members caused their PII/PHI to be compromised in the Data Breach.

146. Plaintiffs and Class members were in no position to protect their PII/PHI themselves.

147. But for Defendant's breach of the duties described herein, Plaintiffs and Class members' PII and PHI would not have been compromised.

148. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII and PHI of its donors and the harm suffered by Plaintiffs and Class members.

149. Defendant's conduct caused the Data Breach, and as a direct and proximate result, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

150. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

151. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

152. Defendant's negligent conduct is ongoing, in that it still holds Plaintiffs' and Class members' PII and/or PHI in an unsafe and nonsecure manner.

153. Plaintiffs and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT II
NEGLIGENCE PER SE
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

154. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

155. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

156. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant of failing to employ reasonable measures to protect and secure PII/PHI.

157. Defendant violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, UCL, CMIA, and CCPA by failing to use reasonable measures to protect Plaintiff's and Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

158. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

159. Plaintiffs and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

160. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

161. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

162. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules, and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

163. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including

but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

164. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

165. Plaintiffs and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class members.

COUNT III
BREACH OF FIDUCIARY DUTY
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

166. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

167. Plaintiffs and Class members gave Defendant their PII/PHI in confidence, believing that Defendant would protect that information. Plaintiffs and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of its donors, which includes safeguarding and protecting Plaintiffs' and Class members' PII/PHI.

168. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the system containing Plaintiffs' and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA and the FTCA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

169. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) substantially increased risks of identity theft and medical theft—risks justifying

expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

170. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

171. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

172. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT IV
BREACH OF CONTRACT
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

173. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

174. Plaintiffs and Class members entered into contracts with Defendant when they obtained medical services, or otherwise provided PII/PHI to Defendant.

175. In exchange for providing medical services, Defendant promised to safeguard and protect the PII/PHI of Plaintiffs and the Class members.

176. Defendant made express promises to Plaintiffs and Class members that:

a. Defendant is "required by law to protect the privacy of health information that may reveal your identity";

b. Defendant will only share information "with your written authorization";

c. Defendant is "required by law to notify affected individuals following a breach of unsecured information"; and

d. Defendant will only share the PII/PHI of its patients in specific scenarios identified in the Privacy Policy and Website Policy.

177. These express promises are contained within Defendant's website and/or other materials provided to Plaintiffs and Class members upon receiving medical services from Defendant.

178. These promises to Plaintiffs and Class members formed the basis of the bargain between Plaintiffs and the Class members, on the one hand, and Defendant, on the other.

179. Plaintiffs and Class members would not have provided their PII/PHI to Defendant had they known Defendant would not safeguard their PII/PHI.

180. Plaintiffs and Class members fully performed their obligations under their contracts with Defendant.

181. Defendant, however, breached its contracts with Plaintiff and the Class members by failing to safeguard Plaintiffs' and Class members' PII/PHI.

182. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

183. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

184. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

COUNT V
BREACH OF IMPLIED CONTRACT
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

185. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

186. In connection with obtaining medical services from Defendant, Plaintiffs and all other Class members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

187. Pursuant to these implied contracts, money was paid to Defendant, whether directly from Plaintiffs and Class members or their insurance carriers, and Defendant was provided with PII/PHI of Plaintiffs and Class members. In exchange, Defendant impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

188. The protection of PII/PHI was a material term of the implied contracts that were either between Plaintiffs and Class members, on the one hand, and Defendant, on the other hand or were between third parties and Defendant to which Plaintiffs and Class members were intended third party beneficiaries.

189. Plaintiffs and Class members or the third parties fulfilled their obligations under the contracts.

190. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

191. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

192. Plaintiffs and all other Class members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII/PHI was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII/PHI has been breached; (vi) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

193. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

194. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

COUNT VI
UNJUST ENRICHMENT
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

195. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

196. This count is pleaded in the alternative to Plaintiffs' breach of contract claims (Counts IV and V).

197. Plaintiffs and Class members conferred a monetary benefit upon Defendant in the form of their sensitive and private information.

198. In exchange, Plaintiffs and Class members should have received from Defendant the services that were the subject of the transaction and should have had their private information protected with adequate data security procedures.

199. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members by acquiring and/or collecting their private information. Defendant appreciated and benefitted from the receipt of Plaintiffs' and Class members' private information in that it used the private information and profited from the healthcare transactions in furtherance of its business.

200. Defendant acquired Plaintiffs' and Class members' private information through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

201. Defendant should not be permitted to retain the PII/PHI belonging to Plaintiffs and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself at the expense of Plaintiffs' and Class members' safety and that were otherwise mandated by federal, state, and local laws and industry standards.

202. Defendant unjustly enriched itself by using the private information acquired from Plaintiffs and Class members to further its business.

203. Notably, Defendant chose not to use any payments to enhance their data security procedures.

204. Had Plaintiffs and Class members known of Defendant's inadequate security measures they would not have provided their PII/PHI to Defendant to collect and maintain.

205. Under principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class members, and should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

206. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

207. Plaintiffs and Class members are entitled to equitable relief as a result of the Data Breach.

COUNT VII
INVASION OF PRIVACY
(Plaintiffs, on behalf of themselves and the Nationwide Class, or in the alternative, the New York Subclass)

208. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

209. Defendant invaded Plaintiffs' and Class members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class members' PII/PHI and by negligently maintaining the confidentiality of Plaintiffs' and Class members' PII/PHI, as set forth in this Complaint. Defendant further invaded Plaintiffs' and Class members' privacy by permitting third parties to access, disclose and publish Plaintiffs' and Class members' PII/PHI online.

210. The intrusion was offensive and objectionable to Plaintiffs, Class members, and to the reasonable person in that Plaintiffs' and Class members' PII/PHI was disclosed without prior written authorization of Plaintiffs and other Class members.

211. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class members provided and disclosed their PII/PHI to Defendant privately with an intention that their PII/PHI would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class members were reasonable to believe that

such information would be kept private and would not be disclosed without their written authorization.

212. As a direct and proximate result of Defendant's acts described throughout this Complaint, Plaintiffs' and the Class members' PII/PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class members suffered damages as described herein.

213. Defendant has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class members' PII/PHI with a willful and conscious disregard of Plaintiffs' and the Class members' right to privacy.

214. Plaintiffs and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Defendant may freely treat Plaintiffs' and Class members' PII/PHI with sub-standard and insufficient protections without intervention by this Court.

215. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs and the Class members great and irreparable injury in that the PII/PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

COUNT VIII
DECLARATORY JUDGMENT
(Plaintiffs, on behalf of themselves and the Nationwide Subclass)

216. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

217. As previously alleged, Plaintiffs and Class were third party beneficiaries of contracts that required Defendant to provide adequate security for the PII/PHI it collected. As previously alleged, Defendant owes duties of care to Plaintiffs and Class members that require it to adequately secure customer data.

218. Defendant still possesses PII/PHI information pertaining to Plaintiffs and Class members.

219. Defendant has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems.

220. Accordingly, Defendant has not satisfied its legal duties to Plaintiffs and Class members. In fact, now that Defendant's lax approach towards data security has become public, the PII/PHI data in its possession is more vulnerable than previously.

221. Actual harm from the ongoing threat of fraud and identity theft has arisen in the wake of the Data Breach.

222. Plaintiffs, therefore, seek a declaration that (a) Defendant's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. engaging third-party security auditors and internal personnel to run automated security monitoring;
c. auditing, testing, and training its security personnel regarding any new or modified procedures;
d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant systems;

e. purging, deleting, and destroying in a reasonable secure manner customer data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps Defendant customers must take to protect themselves.

COUNT IX
VIOLATIONS OF NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES N.Y. GEN. BUS. LAW § 349
(Plaintiffs on behalf of themselves and the Nationwide Class or, alternatively, the New York Subclass)

223. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

224. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

225. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

226. Defendant stored Plaintiffs' and the Class members' PII/PHI data in Defendant's electronic databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiffs' and the Class members' PII/PHI secure

and prevented the loss or misuse of Plaintiffs' and the Class members' PII/PHI. Defendant did not disclose to Plaintiff and the Class members that their data systems were not secure.

227. Plaintiffs and the Class never would have provided their sensitive and personal Private Information if they had been told or knew that Defendant failed to maintain sufficient security to keep such PII/PHI from being hacked and taken by others, and that Defendant failed to maintain the information in encrypted form.

228. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the Class members' PII/PHI.

229. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiffs and the Class members of the Security Breach. If Defendant had complied with these legal requirements, Plaintiffs and the other Class members would not have suffered the damages related to the Security Breach.

230. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that, inter alia:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiffs and the Class at the time they provided such PII/PHI that Defendant did not have sufficient security or mechanisms to protect PII/PHI;

b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security systems that they maintained to protect Plaintiffs' and the Class's PII/PHI.

231. Plaintiffs and the Class were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII/PHI safe. Defendant did not disclose at any time that Plaintiffs' and the Class's PII/PHI was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which they had a duty to disclose.

232. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Security Breach timely and adequately.

233. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

234. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her PII/PHI to Defendant. Said deceptive acts and practices are material. The requests for and use of such PII/PHI in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

235. Defendant's wrongful conduct caused Plaintiffs and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII/PHI materials by third parties and placing Plaintiffs and the Class at serious risk for monetary damages.

236. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

237. In addition to or in lieu of actual damages, because of the injury, Plaintiffs and the Class seek statutory damages for each injury and violation which has occurred.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 21, 2025

Respectfully submitted,

By: */s/ Nicholas A. Migliaccio*
Nicholas A. Migliaccio
nmigliaccio@classlawdc.com
Jason S. Rathod*

jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302,
Washington, DC, 20002
Office: (202) 470-3520

Beena M. McDonald*
bmm@chimicles.com
Alex M. Kashurba
amk@chimicles.com
Marissa N. Pembroke*
mnp@chimicles.com
Samantha Barrett*
sb@chimicles.com
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

**pro hac vice* to be submitted

Counsel for Plaintiff and the Proposed Class